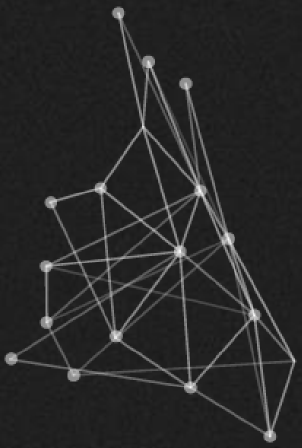
Brought to you by Blockcube Limited.
Blockcube is a Blockchain Consulting, Research & Development Firm.

Telecom on Blockchain

The Telecom Commercial Communication Customer Preference Regulation 2018



blockcube

Consulting

We are harnessing the power of Blockchain technology to revolutionize the everyday world. We provide Blockchain powered solutions to major industry players.

Research

We create the transformational technologies and expertise to operationalize intelligent decisions w.r.t. Blockchain.

Analytics

Using the latest in research technologies, we uncover rich insights so our clients can make more informed decisions.

Blockchain improves coordination between Partners,
with Shared view of Transactions and Liabilities.

Advent of Blockchain in Telecom

What’s Inside ?

01. About Blockcube
- What we do?
  How we do? & Why we do?

02. Blockchain / DLT
- Digital Ledger Technologies
  – a Scalable Alternative

03. Core Product
- TCCCPR 2018 Compliance with
  Improved Efficiency

04. DL-Entity
- Registration and Management
  of Telemarketers

05. DL-Consent
- Adaptable Preferences and
  Consent Register

06. DL-Complaints
- Decentralized Spam, Frauds
  and UCC Reporting

07. Audits and Records
- Auto-Report Generation
  and Maintenance

08. UCC Detect System
- Prevention, Honeypots
  and Tracing

09. Extras
- Silent Calls Detection, Billing
  Ledger & DL-User etc.

10. Value Proposition
- Cost Benefit and Market Value

01. About Blockcube

We are harnessing the power of Blockchain technology to revolutionize the everyday world. We provide Blockchain powered solutions to industries like healthcare, e-governance, finance, supply-chain, defence, media, advertisement and more to count.

01. Blockcube At Your Service

Blockcube is one of the leading Blockchain Research and Consulting company with 8+ years experience. We build, train, advise and research.

Certifications and Record of Rights

Electronic Health Records

Loyalty & Reward Points

Supply Chain

We help manage complex and non-integrated chain to create efficiency, trustless authenticity & end-to-end traceability.

Fund Flow Management

Data Access Management (Contracts and KYC)

Telecom

Blockchain efficiently handles various challenges involved in OSS/BSS processes

Artificial Intelligence & Machine Learning

02. Our Methodology

There is potential for Blockchain to remove intermediaries, or otherwise reduce business-process friction where centralised functions act as bottlenecks.

01

Research

We create best Blockchain Market and Feasibility Analysis.

02

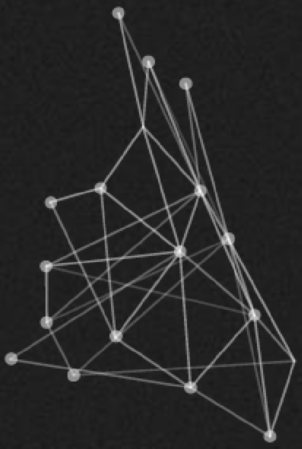
Consulting

We advice and consult businesses keen on Sustainable Growth

03

Development

We develop Blockchain



01

About Blockcube

What is Digital Ledger Technology ?

With 8+ years of Blockchain Expertise, we have helped advance the industry to where it stands now. Our founders have been contributors in renowned projects like Bitcoin Core, Ethereum and Hyperledger.

Bitcoin Core

DIGIHOLO.IO

ethereum

HYPERLEDGER
GENERAL MEMBER

MediLocks
Decentralized Health-Care

Crime Ledgers

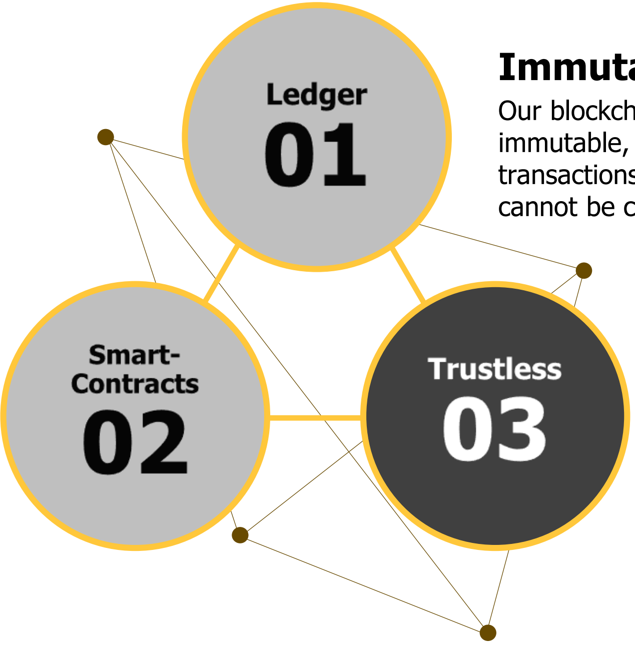
PlugSeal
Decentralized Notary

RDNANCER

02. Blockchain / DLTs

How Blockchain Works?

Blockchain provides an ex-ante enforcement of technical rules, thereby reinforcing the opportunities of regulation by code and the corresponding legal implications it might entail.



Immutability

Our blockchain is fundamentally immutable, because transactions recorded within it cannot be changed/tampered.

Irrevocable

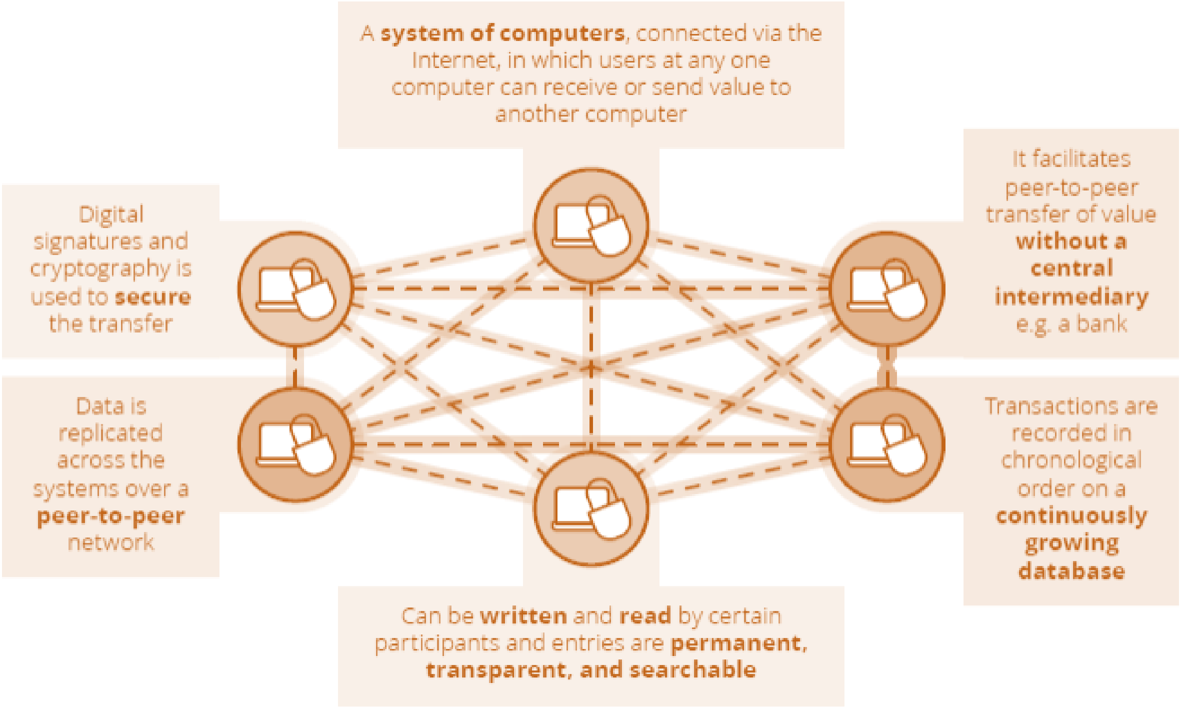
We create irrevocable transactions and processes, in which preset processes can be executed trustlessly.

Auditability

Blockchain relies on its integrity, easy to verify process using Zero Knowledge Proof.

01. How Blockchain Works

Blockchain is a consensus-driven, peer-to-peer network of secure and decentralized nodes forming a distributed ledger, with each node having simultaneous access to transactions updated in the ledger.



A **system of computers**, connected via the Internet, in which users at any one computer can receive or send value to another computer

Digital signatures and cryptography is used to **secure** the transfer

It facilitates peer-to-peer transfer of value **without a central intermediary** e.g. a bank

Data is replicated across the systems over a **peer-to-peer** network

Transactions are recorded in chronological order on a **continuously growing database**

Can be **written** and **read** by certain participants and entries are **permanent, transparent, and searchable**

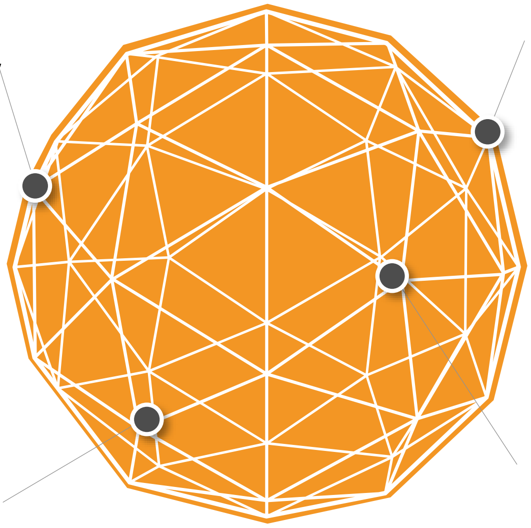
02. Blockchain / DLTs

What is Delegated Proof of Process?

Delegated Proof of Process is our Patent Pending Consensus algorithm which is used to create fault tolerance and efficiency between the distributed nodes.

02. Delegated Proof of Process Blockchain

Our Patent Pending Permissioned Blockchain based on Delegated Proof of Process, where every transaction hash will correspond to a uniquely identifiable successful process mapped to a transaction hash acting as a Zero Knowledge Proof.



Authenticity using
Zero Knowledge Proof

Without sharing any secret behind the transaction, but the key factual elements to enable the proof (digest, signature, public key and the trusted timestamp) where any verifier can validate the integrity..

Provenance and
Contextual Proofs

By cryptographically linking hash of previous step, we establish a clear and provable provenance, and thus create context to even disconnected data. Thus, we have chain of cumulative proofs to ensure the contextual proof.

Interoperability using
Permissioned Access

DPoP allows data exchange between stakeholders with real-time efficiency due to contextual understanding and trustless integrity.

Scalable and
Adaptable Consensus

Any step can fork into multiple branches without any need to reconcile. As time always moves one direction, there can never be circular steps within the same branch.

03. Proof-of-Process Consensus

Proof of Process enables supervisors to trust a typical process by disassociating the proof of data from the real source of data manifestation in a way that yields a solitary proof that can guarantee the process.

Hashing
01

Time Stamp
02

RSA Signature
03

Validation
04

All Process Nodes function and communicate Independently and trustlessly. The final validation is done by Delegated Registered Nodes

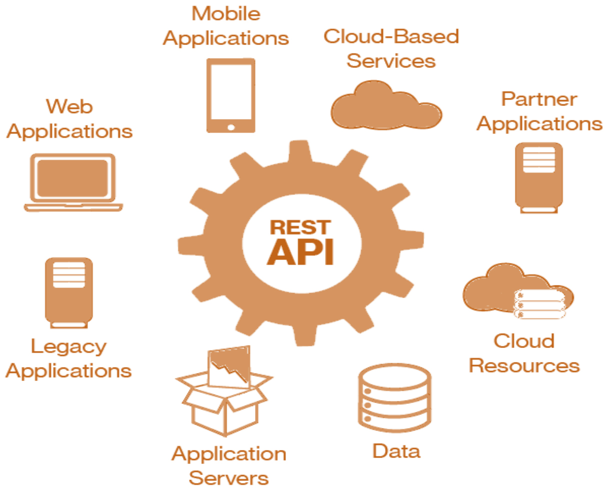
02. Blockchain / DLTs

Technology Behind The Wrappers

Our Interfaces will be an overlay network i.e network that is built on top of another network.

04. Interfaces

All the products work in parallel in sync using DPOP Context Processing. Though there are multiple easy to use interfaces for various stakeholders like CPRF, CCRF, Content Validator API, Monitoring And Reporting System for TRAI, Access Provider System Customer Service Interface, Access Provider System Maintenance Interface, Tele-Marketers Management, Mobile/Web App and many more using various perfectly compatible libraries of Python, C++, Go, Node Js, AngularJs and various custom process adapters.



Remote Procedural Call

Remote Procedure Call (RPC) will allow use of functions/ service from a program located outside the connected infrastructure.

REST APIs

JSON Web Token based Representational State Transfer APIs are created for hassle-free integration relaying all DLT data

MongoDB / FoundationDB

NoSQL databases are especially useful for working with large sets of distributed data. NoSQL usually is best horizontally scaling Database with features like sharding

05. Authorized Applications

The Mobile Applications is a hybrid and has been compiled in **Windows, iOS and Android**.
The Web Interface uses the very scalable NodeJs at the backend, and AngularJs based responsive application.

01. AI/ML Behind App

The Mobile/Web Application is a great store of customer data. We use Geo-location, mapping to KYC, nearby preferences and then learn from your previous experience in regards to RTMs. This automatically creates a continually evolving recommendation engine for the customer.

02. Easy to Use Interface

The UI has a drag n drop Preference Selection functionality with Tinder-Swipe Categorization. All functions can be easily accessed from Navigation Panel.

02. Blockchain / DLTs

P2P approach could save 60% in Bandwidth Costs.

Simplifying, Evolving, and Connecting proven Techniques (like BitTorrent and Git) into a Single Cohesive System

06. Data Transfer Protocol

Our P2P data transfer system is built on a more secure and efficient modified IPFS for versioned data sharing. We provide a high throughput content-addressed block storage model, with content addressed hyper links. This forms a generalized Merkle DAG upon which blockchains, and our data communication protocol works.

We provide historic versioning (like git) and makes it simple to set up resilient networks for mirroring of data.

Versioned Data Transfer

Delegated Validator Nodes

Only delegated nodes can append a new transaction to the Mainnet.

Our nodes have persistent availability with or without Internet backbone connectivity.

Resilient Infrastructure

Your Data is Secured

Our Protocol has no Single Point of Failure, and nodes do not need to trust each other.

07. File Transfer and Data Communication

Each network node stores only content it is interested in, and some indexing information that helps figure out who is storing what. We combines a distributed hashtable, an incentivized block exchange, and a self-certifying namespace.

HTTP is inefficient and expensive

Each file and all of the blocks within it are given a unique fingerprint (Hash). We remove duplications across the network and track version history for every file. When looking up files, you're asking the network to find nodes storing the content behind a unique hash.

Proposed Product

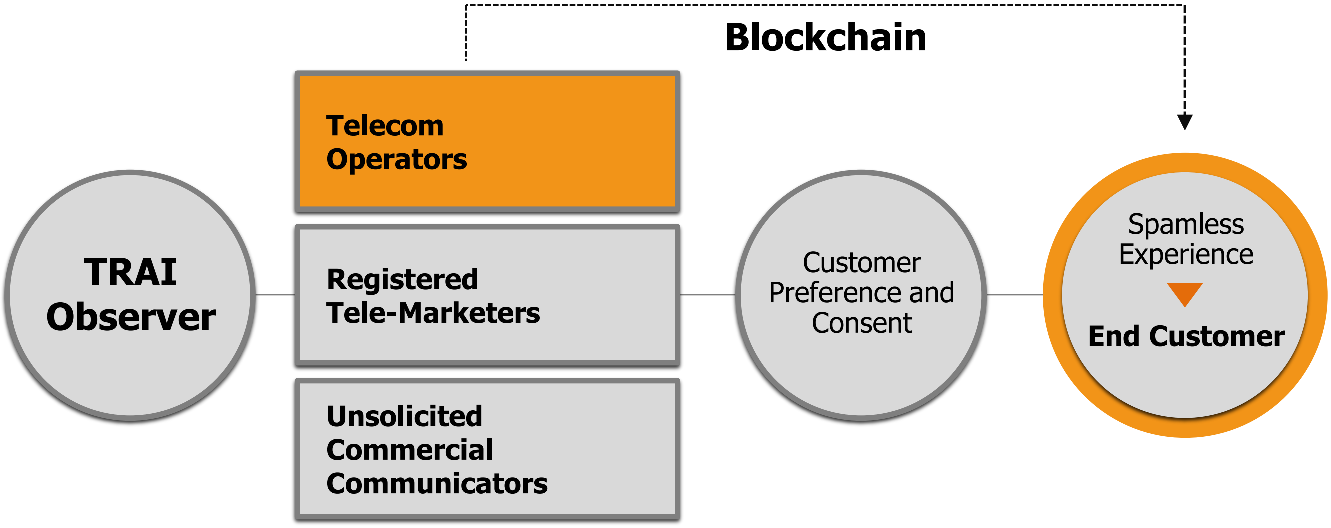
Product Proposed

Blockchain Meets Telecommunication

Implementation of Blockchain in the Telecom Industry can bring about enormous benefits with its efficiency and interoperability.

01. Telecom Customer Preference Regulation Compliance 2018

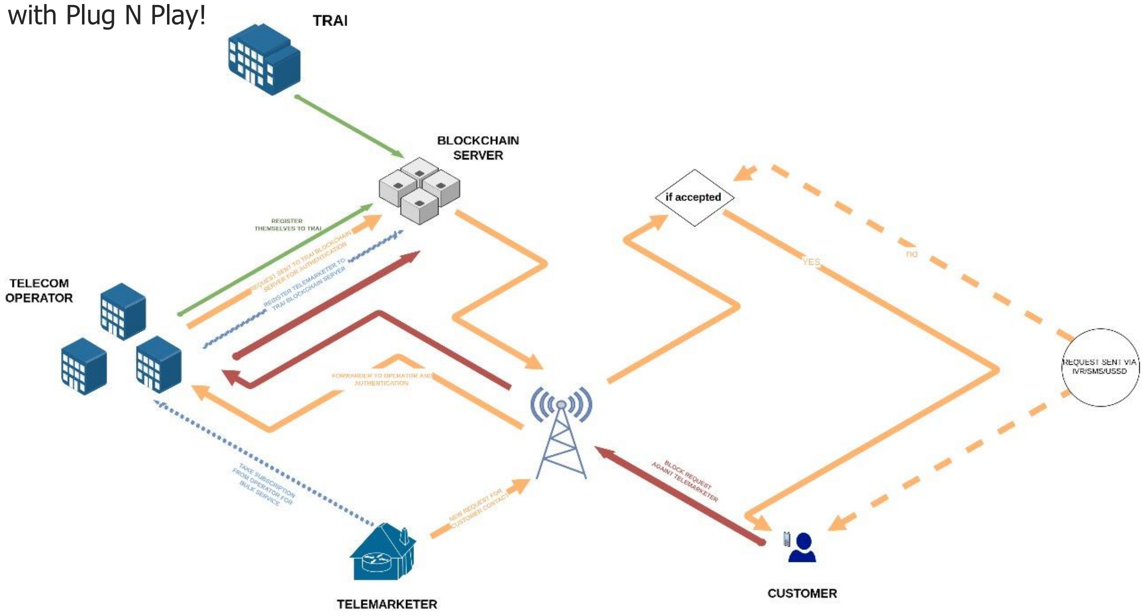
Telecom operations are really complex and there are a lot of trust issues and transparency challenges due to the involvement of multiple entities, and no clear mechanism to track end-to-end activities of every entity. This makes monitoring really difficult for TRAI in case of frauds/spams and other mismanagements. Our product in completely TRAI TCCCRP 2018 compliant and further their infrastructure more efficient.


Blockchain
TRAI Observer
Telecom Operators
Registered Tele-Marketers
Unsolicited Commercial Communicators
Customer Preference and Consent
Spamless Experience
End Customer

This product leads to AI/Machine Learning based systems to detect Fraud/UCC and other silent and automated robo-calls.

02. Blockchain as a Infrastructure

Blockchain is not a software, its an interconnected decentralized infrastructure. We help you literally add new modules with Plug N Play!

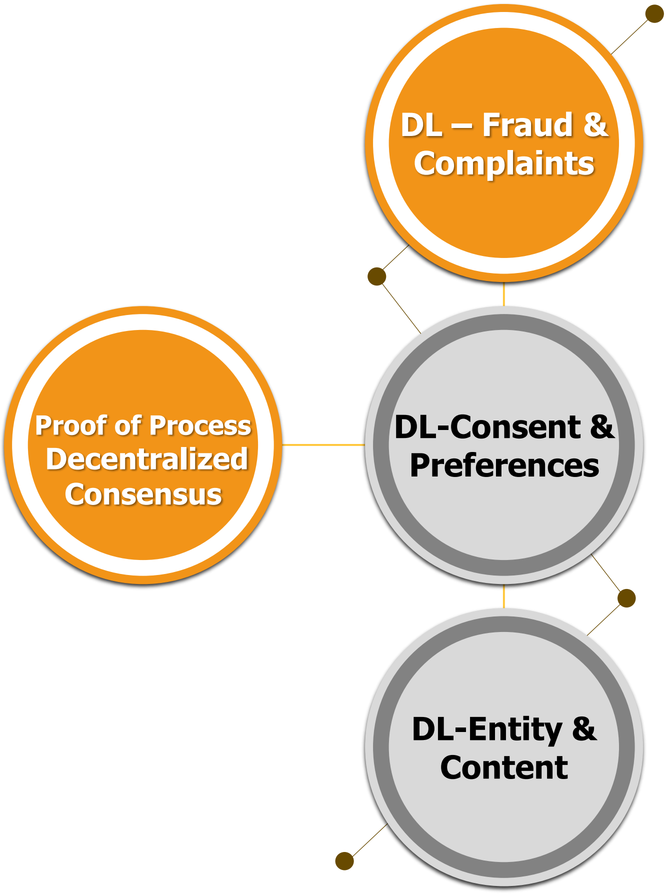

TRAI
BLOCKCHAIN SERVER
REGISTER THEMSELVES TO TRAI
REQUEST SENT TO TRAI BLOCKCHAIN SERVER FOR AUTHENTICATION
REGISTER TELEMARKETER TO TRAI BLOCKCHAIN SERVER
TELECOM OPERATOR
FORWARDER TO OPERATOR AND AUTHENTICATION
if accepted
YES
no
REQUEST SENT VIA IVR/SMS/USSD
TAKE SUBSCRIPTION FROM OPERATOR FOR BULK SERVICE
NEW REQUEST FOR CUSTOMER CONTACT
BLOCK REQUEST AGAINT TELEMARKETER
TELEMARKETER
CUSTOMER

Proposed Products

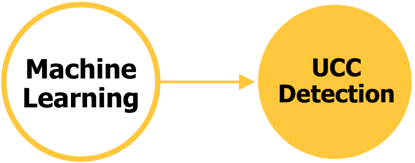
Telecom operations are really complex and there are a lot of trust issues and transparency challenges due to the involvement of multiple entities, and no clear mechanism to track end-to-end activities of every entity. This makes monitoring really difficult for TRAI in case of frauds/spams and other mismanagements.

01. DLT Network Management

The Entire Product/Regulation is a Overlay Network over the foundation of our DPoP Blockchain and Sidechain systems working interconnected with each other.



Used to record Customer / Analysis **Complaints and Reports** regarding violation of Regulations made by the customer in an immutable and non repudiable manner using Customer Complaint Registration Facility.



Used to record **Consent** or record **Revocation** of users consent related to Commercial Communication and change or exercise his preference(s) from the list(s) using Customer Preference Registration Facility.

Google play

To register **Entities** declared by access provider(s) together for various functions and registers like Headers, Content Template Register and Verification, Scrubbing Register and many more. The Telemarketer will furthermore get access to management portal.

02. Other Prime Features

Our Products includes Easy to Use Migration Facility, UCC Prediction and Detection Systems, Silent/ Abandoned Calls Detection, Geographic Relational Structuring,

UCC Prediction and Detection System

Learning from evolving user patterns and signature(s) over time; Access Interface to exchange data with DLT of other access provider(s) to detect sender and revaluating analysis of DL-Complaints.

Automated Migration Facility

Migration plan for existing data, process and role being played at present by different entities to the new system of data, process and role of new entities can be done just in a few clicks.

DL-Entity

Entity Registration Facility

Our easy to use and functional search engine helps you locate the right templates quickly saving your time.

01. Digital Ledger - Entity

Entity Registration Functionality using DLT:

(1) All entities - Telemarketer with associated functions, who will be carrying out given functions for effective control of Unsolicited Commercial Communications being delivered through them, shall be declared using this permissioned Blockchain built on our proprietary Proof of Process which can also be used to declare Telemarketer details;

(2) We help telemarketers carryout one or more functions while keeping all records and execution of functions separately against each activity for internal audit by the Telecom Partners to ensure the effectiveness of Unsolicited Commercial Communications control to meet regulatory outcomes specified in the regulations;

(3) Each functional entity registered in the DL-Entity shall be given unique identity (Key-Pair) by the Telecom Partners to be used to authenticate and track the events

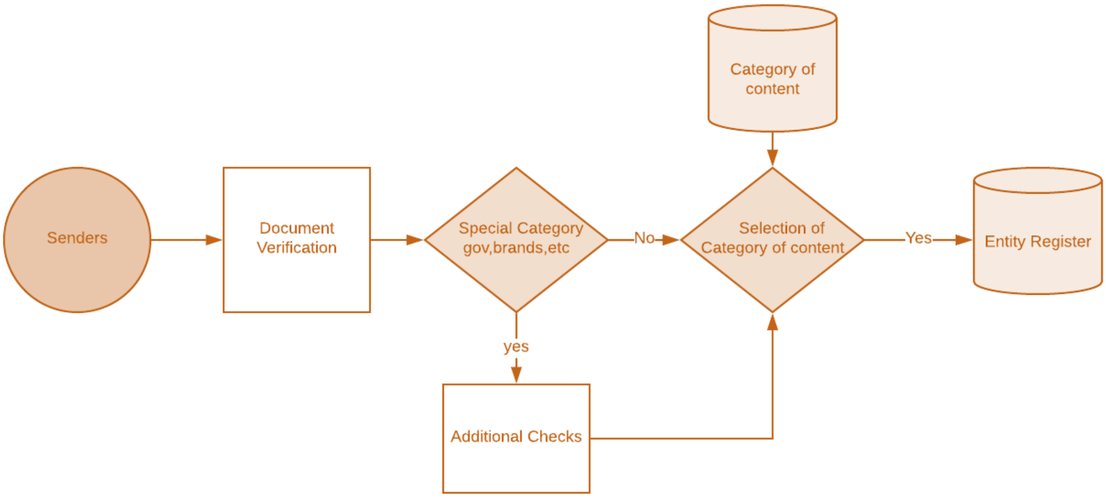
Case Benefit

Using a blockchain ledger to manage identities would make it extremely difficult for fraudsters to wreak havoc without leaving an obvious digital trail. Blockchain enables the secure exchange of cryptographically-signed credentials to prove an owner's identity. The entity record is immutable, meaning that changes to every single identifier associated with an individual must be logged. This prevents malicious actions by data custodians, and ultimately makes identity theft more difficult to execute.

Through an easy registration processes, the business will be able assert their identity and build trust of the clients. This diminishes the ability of unknown entities reaching their customers with calls and messages that are fraudulent or otherwise of dubious nature.

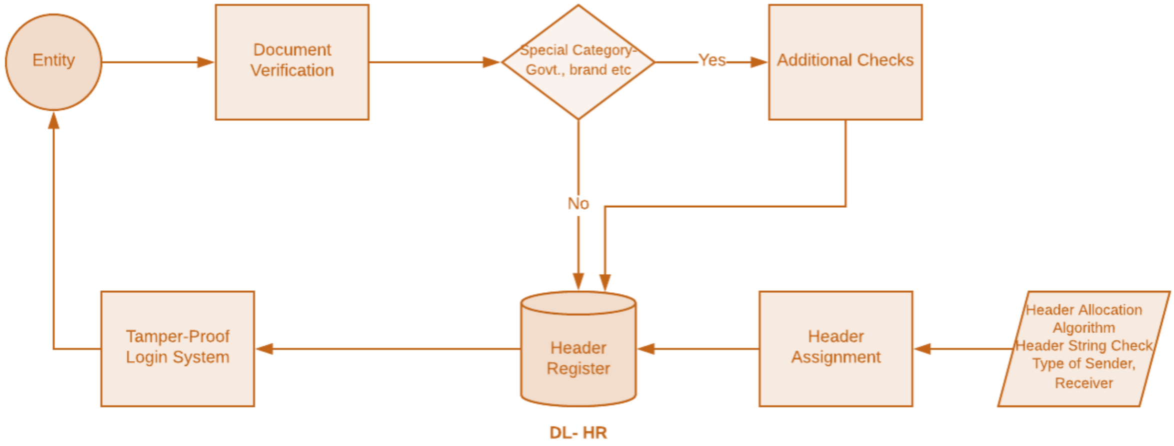
02. Modular Entity Registration Process

Details of all the parties involved in sending commercial communication to the customers are stored in the blockchain – DL-Entity-Register.



03. Header Registration Function (HRF)

Using headers intelligently to segregate different types of messages, businesses shall be able to help their clients manage, delete or store communications related to OTP's, balance enquires, flight alerts, special offers, etc.
Blockchain cryptographically secures the unique headers with their corresponding business. Wih a robust header allocation algorithm, the solution ensures header's uniqueness and easy management.


Entity
Document Verification
Special Category-Govt., brand etc
Yes
Additional Checks
No
Tamper-Proof Login System
Header Register
Header Assignment
Header Allocation Algorithm Header String Check Type of Sender, Receiver
DL- HR

04. Entity Data Life Process

Header Registration Functionality as per allocation and assignment principles and policies, uses API to initiate HRF in DL-Entity.

All carried out pre-verifications of documents and credentials submitted by an individual, business entity or legal entity requesting for assigning of the header are Hashed and stored.
Map Tree of mobile device and mobile number(s) related to the RTM, in a secure and safe manner, which shall be used subsequently on regular intervals for logins to the sessions by the header assignee.
Carry out additional checks for look-alike headers which may mislead to a common recipient of commercial communication, it may also include proximity checks, similarity after substring swaps specifically in case of government entities, corporate(s), well-known brands while assigning headers.

Record customer consent via Customer Consent Acquisition Functionality on Consent Register, using REST APIs of the facility to take agreement to the purpose of consent and details of sender and authenticate customer giving the consent through OTP.

DL-Entity-Content

Content Registration and Verification

Our easy to use and functional search engine helps you locate the right templates quickly saving your time.

05. Digital Ledger – Content Template

Entity Content Registration Functionality using DLT uses simple REST APIs:

- Categorize Content Templates
- Identify fixed and variable portion(s) of the content in the offered transactional template and service message template with identification of type of content for each portion of variable part of the content, e.g. date format, numeric format, name of recipient, amount with currency; reference number, transaction identity;
- To de-register template or temporarily suspend use of template;
- Transaction hash is generated for fixed portion of content of template upon confirming the template and assigning unique template identity to registered template of content;

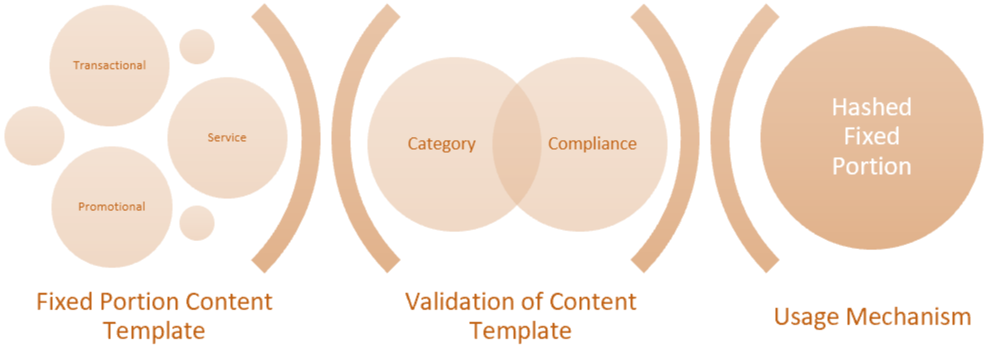
Case Benefit

The content record is immutable alongside the DL-Entity in a sidechain which records the identity, meaning that changes to every single identifier associated with the content is logged. This also makes content validation across telecom operators efficient, something where they typically have little or no direct access to information about interactions that a client may have had with other public authorities. And collecting such information can be a painstaking effort, requiring lots of time and legwork.

Through an easy content registration process, the business will be able assert their standardized content and are also free from any mischievous acts or mistakes by data custodians. This lessens the risk of unknown content reaching their customers with calls and messages that may hamper their business. This process also efficiently automates their communication which is auditable.

06. Content Template Registration

Records for RTM approved SMS/Call templates, out of which only they can send commercial communication to the preferred and scrubbed customers are stored in the blockchain – DL-Entity-Content.



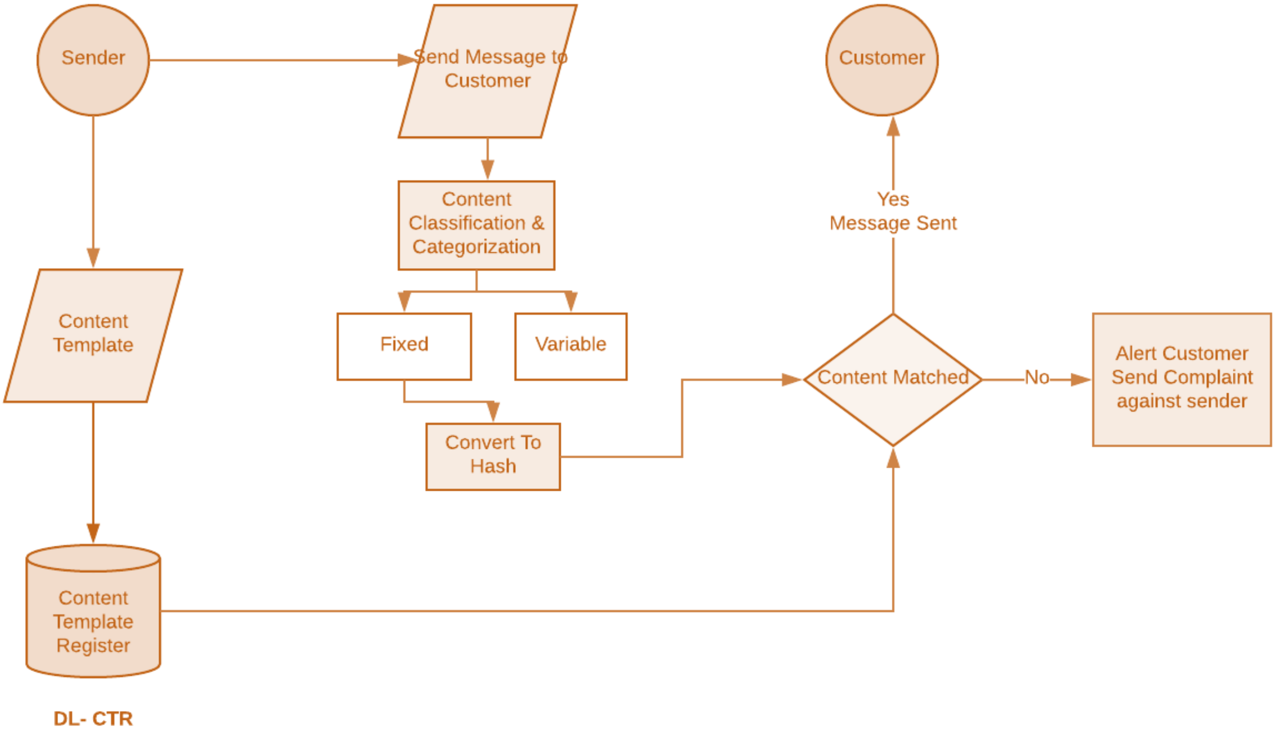
07. Content Verification and Validation

The content type and category of messages is identified using a Reference Table and Regressive Analysis when the content is to be delivered or already delivered via an automated tool or utility software.

Telecom operations are really complex and there are a lot of trust issues and transparency challenges due to the involvement of multiple entities, and no clear mechanism to track end-to-end activities of every entity. This makes monitoring really difficult for TRAI in case of frauds/spams and other mismanagements.

Case Benefit

The concept of registered templates for both SMS and voice communication has been introduced to prevent deliberate mixing of promotional messages into the transactional stream. This will give relief to subscribers who feel targeted by unwanted communication today. Our solution will efficiently analyse and identify different categories of SMS spam. The content is parsed and processed according to the standard unigram based text clustering practices.

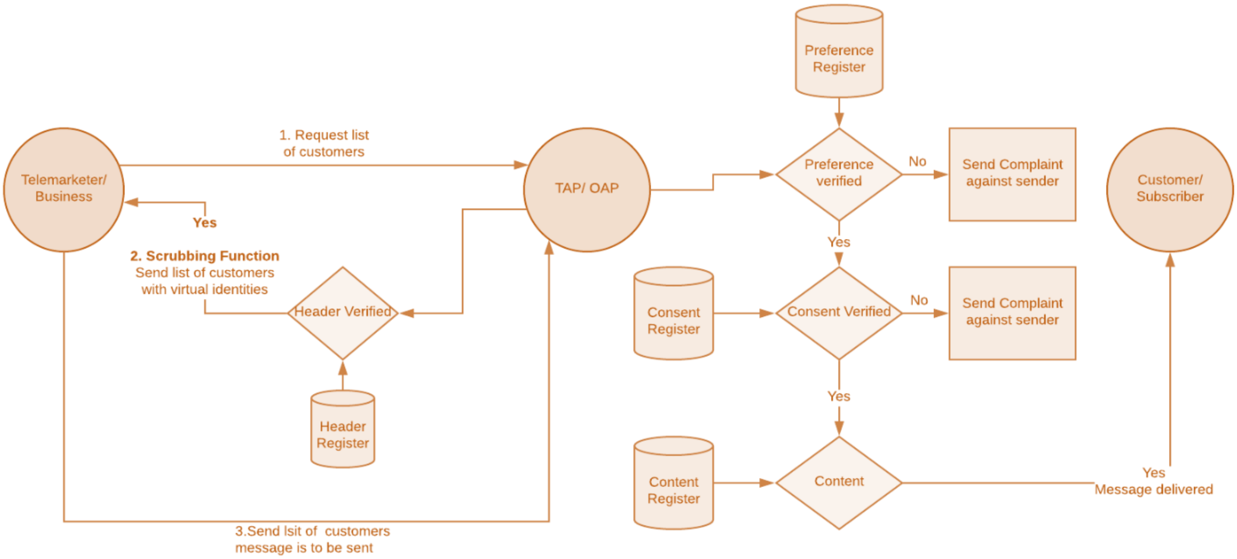


DL-Consent

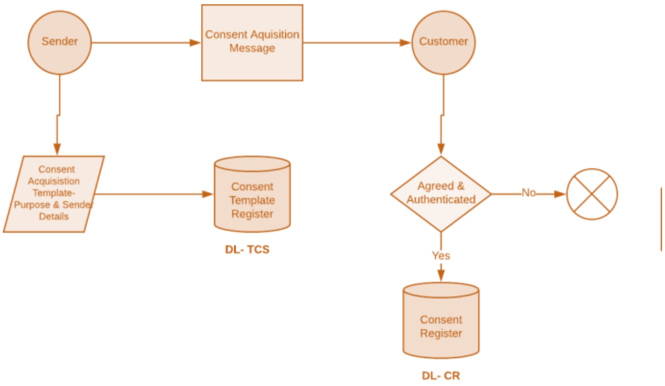
Consent vs Entity DLT

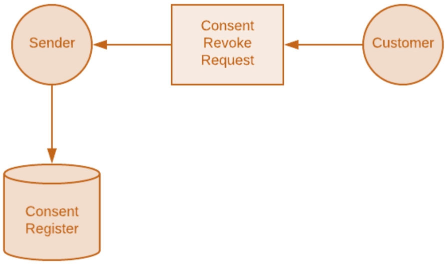
01. Scrubbing as a Service

The solution carries out the scrubbing function in a secure and safe manner. A business requests telecom operator for a list of customers to target and send commercial message. The telecom operator generates a list with virtual identities and share it with the sender without disclosing real identities to any other entity than authorized to know it. The business provide scrubbed list to corresponding telecom operator for carrying out reverse mapping of virtual identities to real identities for further delivery. The message is only delivered if the customer preference, consent matches.



02. Consent Register/Revoke API using OTP


Sender
Consent Aquisition Message
Customer
Consent Acquisistion Template- Purpose & Sender Details
Consent Template Register
DL- TCS
Agreed & Authenticated
No
Yes
Consent Register
DL- CR



DL-Consent

Consent/Preference Registration Facility

03. Digital Ledger - Consent

Record, following details of the customer who has registered its preference(s) using 1909 or mobile/web app:

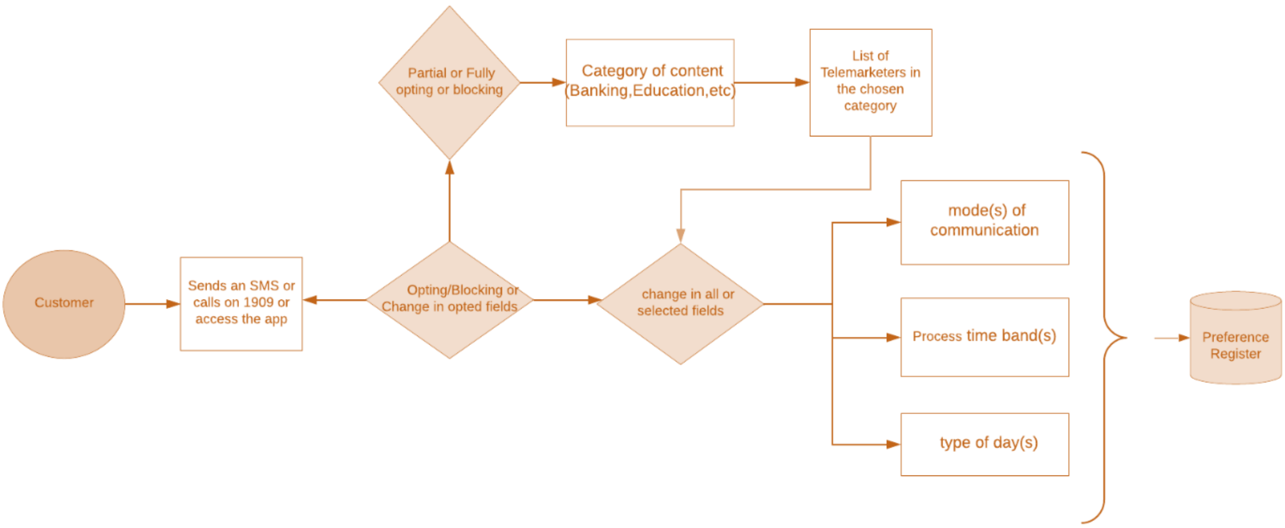
- Telephone number as in National Numbering Plan;
- Location Routing Number (LRN), as assigned by DoT to the access provider, of current serving
- network of the customer and changes in LRN of the new serving network, in case customer is being
- ported-in during Mobile Number Portability;
- His preference(s) and subsequent changes to it made by the customer from time to time;
- Changes in the subscription of telephone number, during the process of opening and closing of
- subscription;
- Unique Registration Number (Stripped Public Key) issued at the time of registration of preference(s)

Case Benefit

Unscrupulous telemarketers today override the stated preference of the subscriber by claiming consent that may have been surreptitiously obtained. New regulations provide the subscriber with complete control over their consent and the ability to revoke the consent already granted, at their option. A major abuse of the current regulations would thus be stopped.
Consent of customers are updated real-time and maintained in Blockchain registers. In case, a customer revokes consent, the ledgers are updated to reflect the same instantly.

04. Modular Entity Registration Process

The solution in sync with the new regulations provide for fine grained control over preferences, including such options as the time window in which to allow specific types of unsolicited communication.


Partial or Fully opting or blocking
Category of content (Banking,Education,etc)
List of Telemarketers in the chosen category
Customer
Sends an SMS or calls on 1909 or access the app
Opting/Blocking or Change in opted fields
change in all or selected fields
mode(s) of communication
Process time band(s)
type of day(s)
Preference Register

DL-Complaints

Customer Compliants Registration Facility

The reports in certain cases may also acts a indisputable timestamped proof by cyber cell as an evidence.

01. Digital Ledger - Complaints

Customer Complaint Registration Functionality using DLT:

- Customer makes a call to 1909 for registering his complaint, network relay call the DL-Complaints APIs.
- When registering via SMS details provided by the complainant regarding date/time on which it was received along with content of received message and in case of voice call, brief of content of communication etc.
- Functioning of intelligent and intuitive mobile app(s) for devices with different operating systems
- and helping customer to identify and report suspected sources of spam and also making use of it
- by the customer to make complaints and the same gets converted to JSON and sent securely across the DL-Complaints RPC Server to be immutable stored
- Procedure for the customer to make complaints by visiting website of access provider and register
- his complaint. Procedure for filling form and design it for the purpose of filing complaint with all relevant details required to investigate complaint and take appropriate action and this further calls DL-Complaints RPC Server APIS to initiate a new Complaint.

02. Augmented Behavior

This system will be used for reporting of unsolicited communication alongside UCC Detect Systems, without which spam control seems difficult as per our opinion. CCRF is intended to be a repository of spammers. The system will use public auditable smart contracts as an alternate to Remote Process Automation.

Fraud Detection		**Augmented Behavior**
Fraud/Ponzi Scheme or any other Cyber Crime when reported at Telecom ops discretion forwarded to Cyber Cell.		Telecom Operators and Cyber Cell Authorities can take actions as per the law, caller ID will be blocked forever.
Unsolicited Call Report if processed but no wrongdoing is concluded.	**DPoP** Blockchain ❯❯❯	The caller will be allowed to access the system again and cleared from Sidechain.
Unsolicited Telemarketer when reported will be scrutinized and found guilty.		Telemarketer will be blocked out of the network and associated KYC will be reported.

DL-Complaints

Complaint Registration Facility

The reports in certain cases may also acts a indisputable timestamped proof by cyber cell as an evidence.

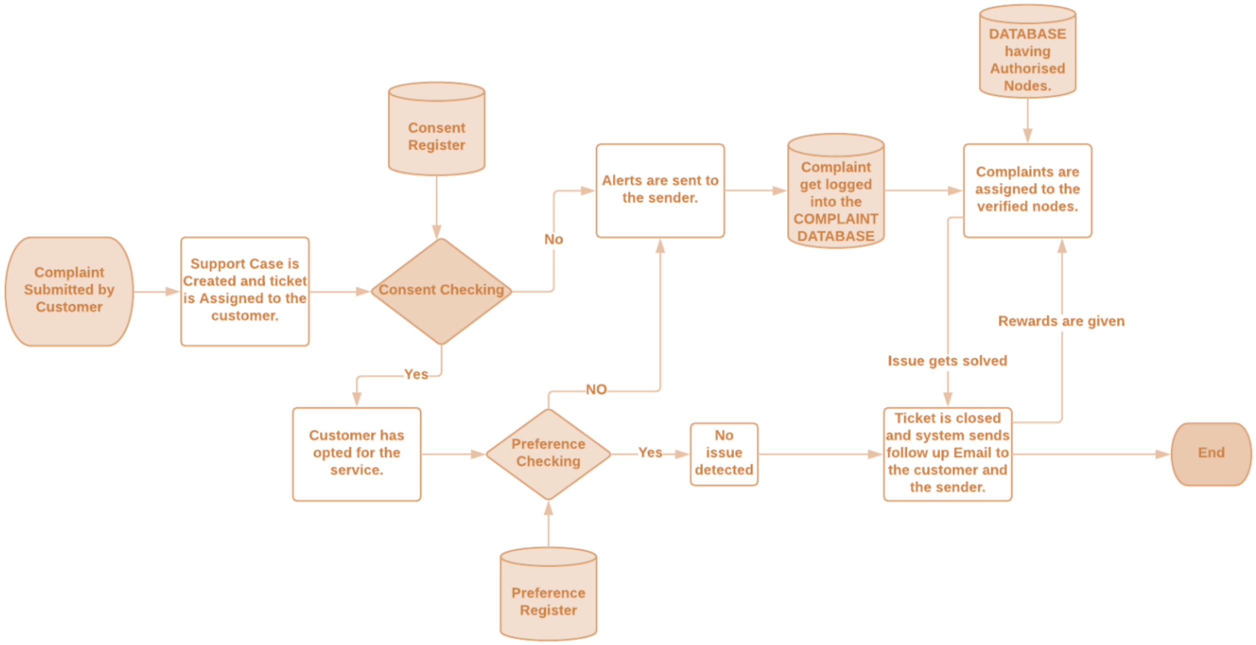
03. Behavioral Augmentation – UTM/RTM – Taking Actions

Terminating Access Provider notifies OAP using DLT. The following processes are mandated by the blockchain process. Lets consider all redressal situations:

(1) UTM- Examine Communication Detail Records;
(2) RTM- Extract Consent Template and Content Template from existing records using DLT Unique Seller Hash. All actions including warnings and issue of notice will be reported in the ledger.
(3) ML/AI and UCC Detect based Usage Cap Restriction can play a major role in cutting down UCC communication.

Case Benefit

The complaints regarding the USCC can be solved in the minimum time, since when ever the customer is facing the problem of unsolicited advertisements, the new technology can provide the ample of authorized nodes that can view and resolve the problem in no time and get rewards for doing so.
Customers may report/mark calls/SMS as a spam/fraud/crime, such a request will be push to a sidechain acting solely to process such malicious attempts. The other party need not be a telemarketer for this process to be initiated. The Proof originating from Blockchain and other UCC Detect Systems will also be accessible by Cyber cell and Telecom Operations.


DATABASE having Authorised Nodes.
Consent Register
Alerts are sent to the sender.
Complaint get logged into the COMPLAINT DATABASE
Complaints are assigned to the verified nodes.
No
Complaint Submitted by Customer
Support Case is Created and ticket is Assigned to the customer.
Consent Checking
Rewards are given
Issue gets solved
Yes
NO
Customer has opted for the service.
Preference Checking
Yes
No issue detected
Ticket is closed and system sends follow up Email to the customer and the sender.
End
Preference Register

UCC Detection

Unsolicitated Commercial Communication

01. UCC Detect System

Standardized Technical Measures to share intelligence information, rules, criteria to detect suspected sources of spams can acquired through our system.

Frauds And Spams

Implementation details for detecting Unsolicited Commercial Communications related to suspicious unregistered telemarketing activity using Signature solution, deploying honeypots and other technical measures.

Silent and Abandoned Calls

Report of entities found to be engaged in making or causing to make silent calls, robocalls, abandoned calls or using telephone directory harvesting software to make Unsolicited Commercial Communications

02. Machine Learning And Artificial Intelligence

We provide add-on modules with Neuro-Linguistic Programming to learn and predict to reduce UCC.

Honeypots, Call Interception etc.

Honeypots, Calls Interceptions are a very secure way to discreetly accumulate data regarding UCC, which may further be needed in of Cyber Cell or other regulatory audits.

Big Data and Machine Learning

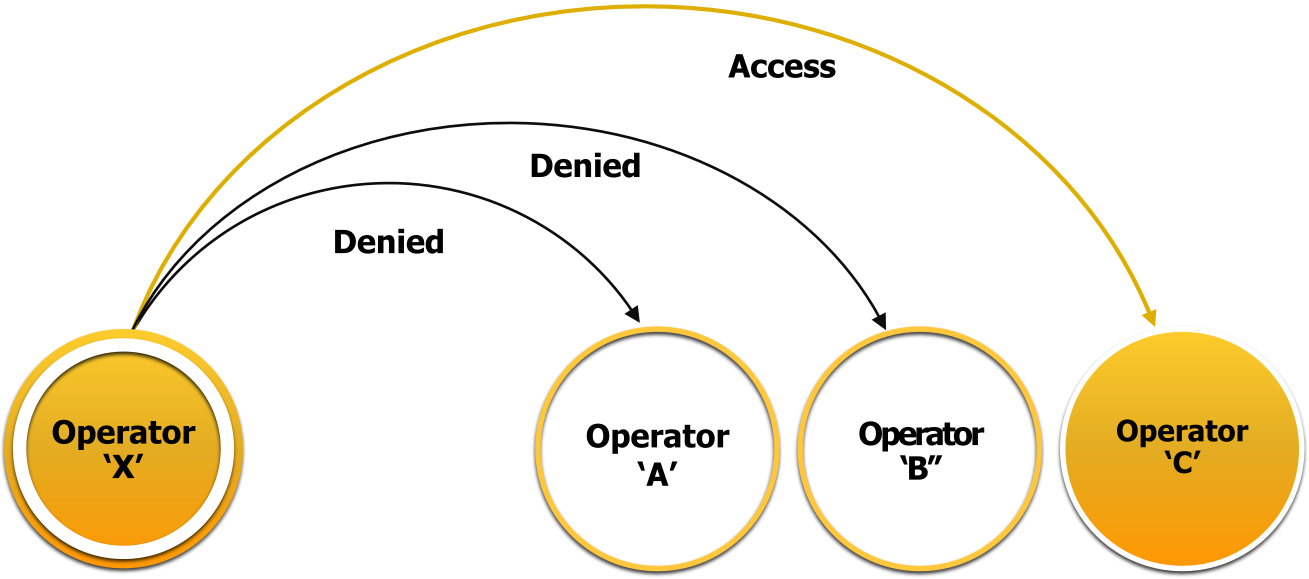
Big Data and ML approaches to detect and identify unregistered Unsolicited Commercial Communications sender(s), who are camouflaging themselves by fragmenting their activity across multiple phone numbers can be efficiently using Geo-Tagged Mobile Clusters.

Extra AddOns

Numerous Benefits to Using Blockchain

01. Mobile Number Portability

The CSP can extend such a blockchain-enabled identity and access solution to provide data storage and verification services to private clients.CSPs could provide blockchain based Identity verification, data management and storage services to both private clients and subscribers.



Permissioned Data Architecture

Block chain as a service can provide a immutable database to store documents of users. Consesus algorithm to do the necessary verififcations needed for the process.

02. Other AddOns

Roaming Errors/Frauds

A permissioned blockchain could be implemented between every pair of operators which have a roaming agreement.

Subscription Identity Fraud

Mobile number acts as unique identification for an individual, serving as a digital identity.

Silent / Abandoned Call Mapping

Audio and Digital Signal Processing Solutions involving Voice Quality Analysis can be used to mitigate these.

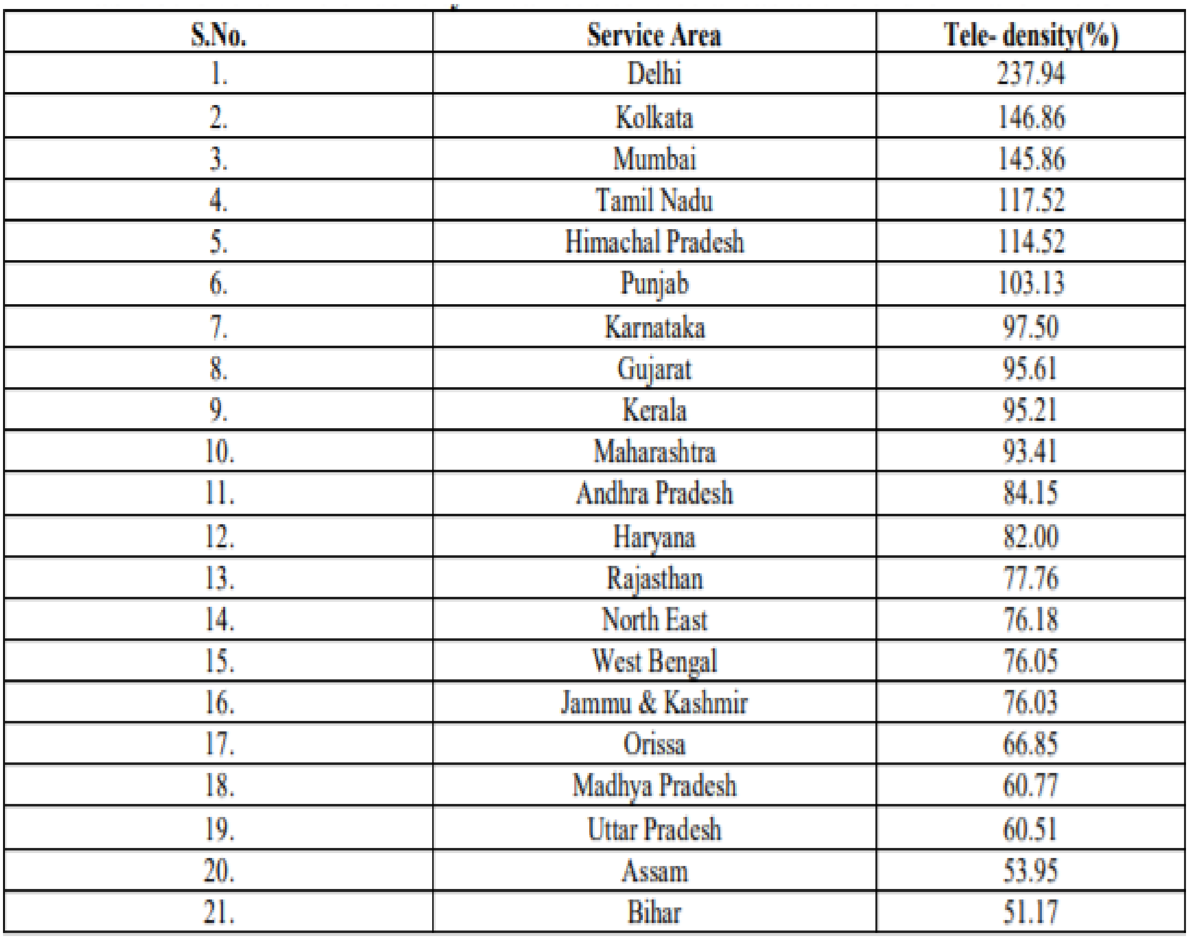
Billing

Telcos could streamline their operational and business processes by adopting hybrid blockchain networks.

Market Analysis

01. Tele-Density

According to TRAI's annual reports of various years, India's tele- density has increased from 18.23% at the end of March 2007 to 78.66% at the end of March 2012. However, tele- density declined from 78.66% at the end of March 2012 to 73.32% at the end of March 2013. This is also indicated in the graph. The graph also depicts that the Urban Tele- density has decreased from 169.55% at the end of March 2012 to 146.96% at the end of March 2013. But Rural Tele- density has increased during the interval. There is a large disparity between the urban tele-density and rural tele-density. The slow growth in teledensity in the rural areas is due to these areas being less attractive for the telecom service providers to invest in. Furthermore, providing telecom services in the remote and rural areas also requires massive investment. Rapid increase in rural tele- density is very important for the economic and social development of rural areas, which will help in the overall development of the whole country. The Government of India has employed several measures for spreading up of mobile network in distant rural areas. Private telecom operators are trying their best to expand their services in rural areas by providing them good services.



S.No.	Service Area	Tele- density(%)
1.	Delhi	237.94
2.	Kolkata	146.86
3.	Mumbai	145.86
4.	Tamil Nadu	117.52
5.	Himachal Pradesh	114.52
6.	Punjab	103.13
7.	Karnataka	97.50
8.	Gujarat	95.61
9.	Kerala	95.21
10.	Maharashtra	93.41
11.	Andhra Pradesh	84.15
12.	Haryana	82.00
13.	Rajasthan	77.76
14.	North East	76.18
15.	West Bengal	76.05
16.	Jammu & Kashmir	76.03
17.	Orissa	66.85
18.	Madhya Pradesh	60.77
19.	Uttar Pradesh	60.51
20.	Assam	53.95
21.	Bihar	51.17

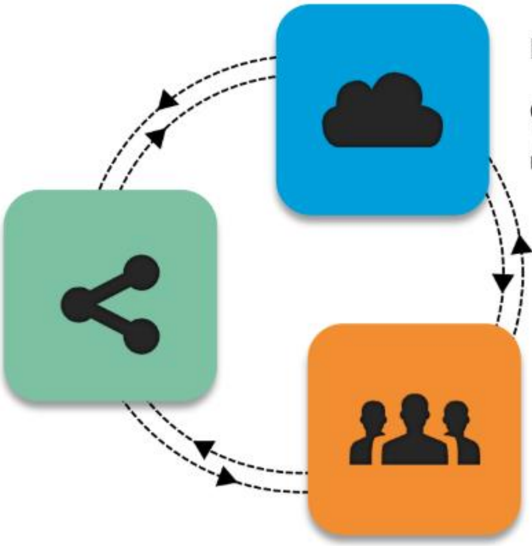
Source: TRAI Press Release 2015

Market Scenario

Market Segmentation

01. Spam Segmentation

With the goal of analysing and identifying different categories of SMS spam, we have performed a clustering experiment on the corpus presented in the previous section. The raw documents were parsed and processed according to the standard unigram-based text clustering practices.



Phishing/Smishing

13.0% of the messages. Considering the reported rise in phishing and smishing attacks in recent time

SMS Spam

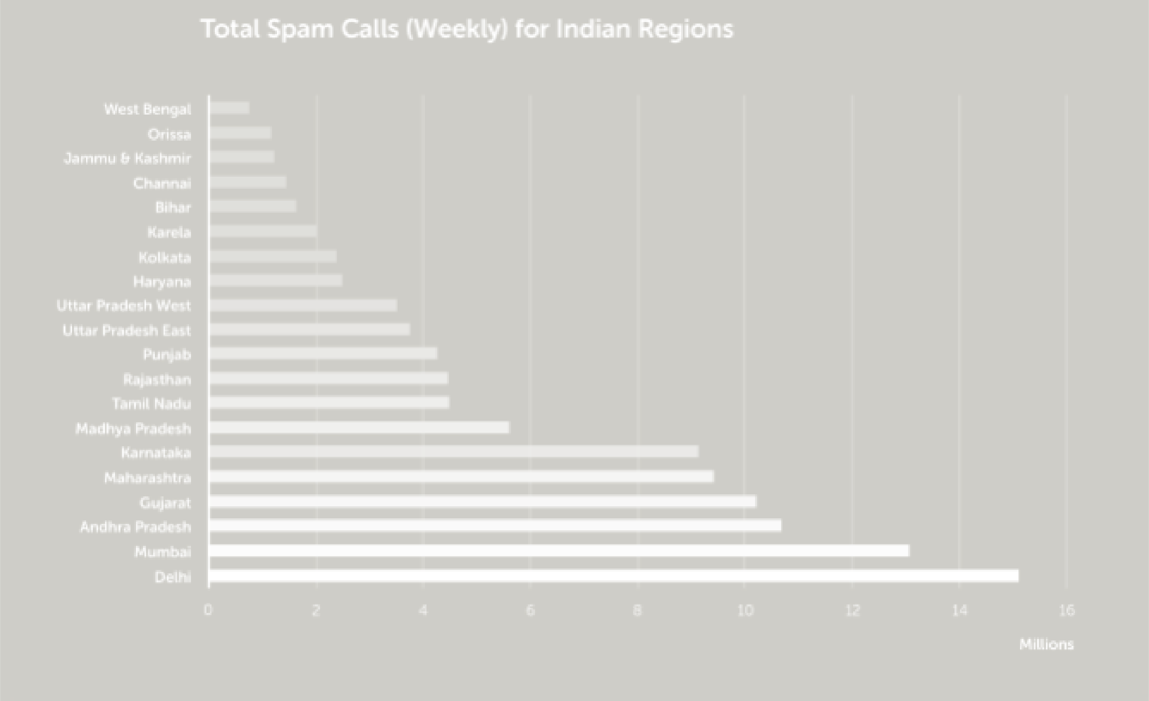
The ringtones and competitions clusters can be categorised as SMS spam and account for **32.4%** of the messages.

Premium rate fraud

clusters claims, prizes, voice mail, dating, and chat, and accounts for **43.9%** of the messages.

02. Geographic Segmentation

Indian callers receive a huge amount of spam calls, more than 300 million per month! Delhi users alone receive a massive 60 million spam calls every month (15 million per week.) So, to ensure that the top spammer list is relevant for each user, we decided to narrow down the list to regional level.

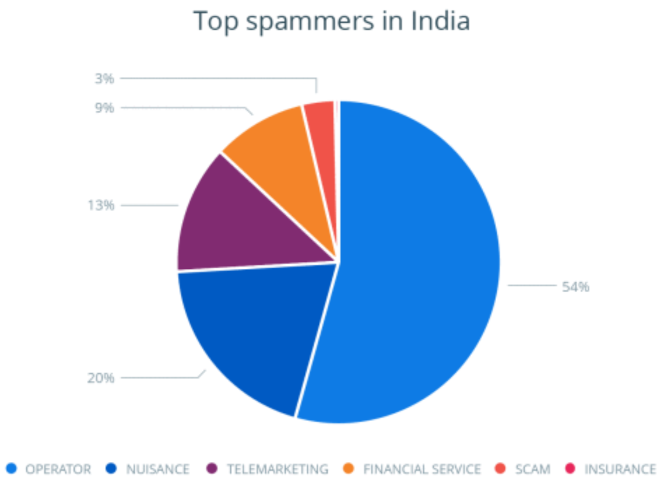


Market Scenario

Market Segmentation

01. Spam Segmentation

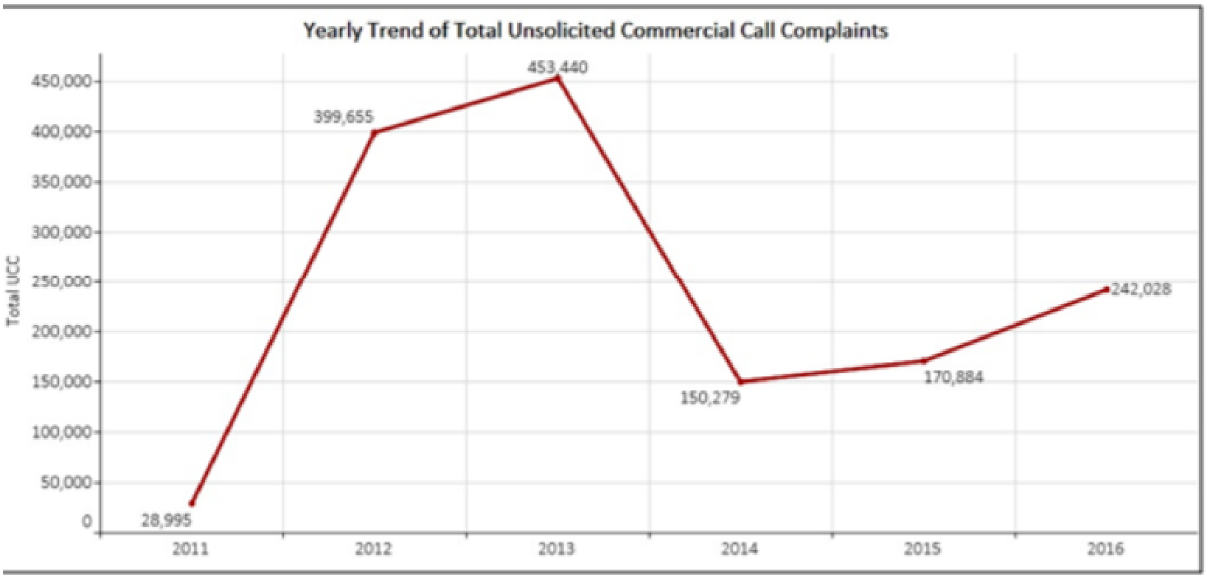
- Operator and Financial companies jointly make up 63% of all spam call that an Indian user received in 2017.
- Nuisance calls (20%): A broad spectrum of calls including unwanted, disturbance for users,.
- Telemarketing spam (13%): Promotional calls from companies, surveys, political/robo calls
- Scam (9%): Fraud attempts, money swindling, unknown links, etc.
- Insurance (3%): Companies selling insurance products and policies.



02. Statistics – Unsolicited Commmercial Communication

According to the Authority, of the 83,908 complaints it received, 40 per cent of the complaints received during October 2017-March 2018 directly led to the disconnection of resources, whereas in a little over 3 per cent of the cases, the agency had already been disconnected or blacklisted (in the case of registered telemarketers) due to complaints by other subscribers.

“Some others have received notices and action is due to be taken in those cases,” said another official at TRAI, adding that around 30 per cent calls were service calls or communication based on previous consent given by the complainant or otherwise wrongly identified by him/her as spam.



Thank you